Roditty-Gershon *Res. Number Theory* (2017) 3:6
DOI 10.1007/s40993-016-0066-2

Research in Number Theory

RESEARCH Open Access

Square-full polynomials in short intervals and in arithmetic progressions

E. Roditty-Gershon*

*Correspondence:
er14265@bristol.ac.uk
School of Mathematics, University of Bristol, Bristol BS8 1TW, UK

Abstract

We study the variance of sums of the indicator function of square-full polynomials in both arithmetic progressions and short intervals. Our work is in the context of the ring $\mathbb{F}_q[T]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q \to \infty$. We use a recent equidistribution result due to N. Katz to express these variances in terms of triple matrix integrals over the unitary group, and evaluate them.

Contents

1 Background

A positive integer n is called a square-full number if $p^2|n$ for every prime factor p of n. Denote by α_2 the indicator function of square-full numbers, i.e.

$$\alpha_2(n) = \begin{cases} 1 & \text{if } n \text{ is square-full,} \\ 0 & \text{otherwise.} \end{cases} \tag{1.1}$$

Springer Open

Let $\mathcal{A}(x)$ be the number of square full integers not exceeding x. In 1935, Erdös and Szekeres [5] proved

$$\mathcal{A}(x) = \frac{\zeta(3/2)}{\zeta(3)}x^{1/2} + O_\epsilon(x^{1/3+\epsilon}). \tag{1.2}$$

Bateman and Grosswald [1] improved this result in 1958. They obtained

$$\mathcal{A}(x) = \frac{\zeta(3/2)}{\zeta(3)}x^{1/2} + \frac{\zeta(2/3)}{\zeta(2)}x^{1/3} + O(x^{1/6}\cdot \mathrm{e}^{-\mathrm{c}(\log^3 \mathrm{x}/\log\log \mathrm{x})^{\frac{1}{5}}}), \tag{1.3}$$

where c is a positive absolute constant. They also made the observation that any improvement of the exponent $\frac{1}{6}$ would imply that $\zeta(s) \neq 0$ for $\Re s > 1-\delta \quad (\delta > 0)$. There is a very long history of studies and conditional improvements (assuming RH) of the error term in the above formula (see [2–4,15,19–22]).

It follows from (1.3) that for intervals of length $H > x^{2/3+\epsilon}$ we have

$$\sum_{x\le n\le x+H} \alpha_2(n) \sim \frac{\zeta(3/2)}{2\zeta(3)}\cdot H/x^{1/2}. \tag{1.4}$$

Various authors used exponential sum techniques to reduce the lower bound on H for which this asymptotic is valid. Heath-Brown [7] proved it with for $H > x^{\eta+\epsilon}$ with $\eta = 0.6318\ldots$ Liu [16] proved it with $\eta = 0.6308\ldots$ Filaseta and Trifonov [6] found a simpler approach, using real instead of complex analysis, and obtained the exponent $\eta = 0.6282\ldots$ In [8], Huxley and Trifonov improve this to $H \ge \frac{1}{\epsilon}x^{5/8}(\log x)^{5/16}$.

Concerning the distribution of square full numbers in arithmetic progressions, the most recent result is due to Munsch [17]. By evaluating character sums, he showed that

$$\sum_{\substack{n\le x\\ n=a \mod q}} \alpha_2(n) \sim \frac{\zeta(3/2)}{\zeta(3)}\frac{A_{a,q}}{q}x^{1/2} + \frac{\zeta(2/3)}{\zeta(2)}\frac{B_{a,q}}{q}x^{1/3}, \tag{1.5}$$

where

$$A_{a,q} = \prod_{p|q}\left(1-\frac{1}{p^3}\right)^{-1}\sum_{\chi\in X_2}\chi(a)\frac{L(3/2,\chi)}{\zeta(3/2)}$$

and

$$B_{a,q} = \prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}\sum_{\chi\in X_3}\bar{\chi}(a)\frac{L(2/3,\chi)}{\zeta(2/3)}$$

with X_2 and X_3 being the set of all quadratic and cubic characters mod q respectively and $L(s,\chi)$ is the L-function attached χ.

The goal of this paper is to study the fluctuations of the analogous sums in the function field settings. Namely, we study the variance of the sum of α_2 in arithmetic progressions and in short intervals, in the context of the ring $\mathbb{F}_q[T]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q\to\infty$. In our setting we succeed in giving definitive results in both cases.

Our approach involves converting the problem to one about the correlation of zeros of a certain family of L-functions, and then using an equidistribution result of Katz which holds in the limit $q\to\infty$.

2 Square-full polynomials

Let $\mathbb{F}_q$ be a finite field of an odd cardinality q, and let $\mathcal{M}_n$ be the set of all monic polynomials of degree n with coefficients in $\mathbb{F}_q$. In analogy to numbers, we say that $f\in\mathcal{M}_n$ is a square-full polynomial if for every polynomial $P\in\mathcal{M}_n$ that divides f, P^2 also divides f. We denote by α_2 the indicator function of square-full polynomials, i.e.

$$\alpha_2(f) = \begin{cases} 1 & \text{if } f \text{ is square-full,} \\ 0 & \text{otherwise.} \end{cases} \tag{2.1}$$

The mean value of α_2 over all monic polynomials is defined to be

$$\langle \alpha_2 \rangle_n := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha_2(f). \tag{2.2}$$

The generating function for the number of monic square-full polynomials of degree n, i.e. $\sum_{f \in M_n} \alpha_2(f)$ is (see [1])

$$\sum_{n=0}^{\infty} \sum_{f \in M_n} \alpha_2(f) u^n = \frac{Z(u^2)Z(u^3)}{Z(u^6)}, \tag{2.3}$$

where $Z(u)$ is the zeta function of $\mathbb{F}_q[T]$ (also set $\zeta_q := Z(q^{-s})$) , given by the following product over prime polynomials in $\mathbb{F}_q[T]$

$$Z(u) = \prod_P (1 - u^{\deg P})^{-1} = \frac{1}{1 - qu}. \tag{2.4}$$

By expanding we have

$$\frac{Z(u^2)Z(u^3)}{Z(u^6)} = \sum_{i,j=0}^{\infty} u^{2i+3j} q^{i+j} (1 - qu^6). \tag{2.5}$$

Therefore, for $n \geq 6$ the coefficient of u^n is given by

$$\begin{aligned} &\sum_{2i+3j=n} q^{i+j} - q \sum_{2i+3j=n-6} q^{i+j} \\ &= q^{n/2} \sum_{\substack{j=n \mod 2 \\ 0 \leq j \leq \lfloor \frac{n}{3} \rfloor}} q^{\frac{-j}{2}} - q \cdot q^{n/2} \sum_{\substack{j=n \mod 2 \\ 0 \leq j \leq \lfloor \frac{n}{3} \rfloor - 2}} q^{\frac{-j}{2} - 3}, \end{aligned} \tag{2.6}$$

which give for $n \geq 6$

$$\sum_{f \in M_n} \alpha_2(f) = \frac{q^{n/2}}{\zeta_q(3)} \sum_{\substack{j=n \mod 2 \\ 0 \leq j \leq \lfloor \frac{n}{3} \rfloor - 2}} q^{\frac{-j}{2}} + q^{\lfloor \frac{n - \lfloor n/3 \rfloor}{2} \rfloor}. \tag{2.7}$$

Therefore in the limit of $q \to \infty$ we get

$$\langle \alpha_2 \rangle_n \sim q^{\lfloor n/2 \rfloor - n}. \tag{2.8}$$

2.1 Arithmetic progressions

Let $Q \in \mathbb{F}_q[T]$ be a squarefree polynomial of a positive degree. The sum of α_2 over all monic polynomials of degree n lying in the arithmetic progressions $f = A \mod Q$ is

$$S_{\alpha_2;n;Q}(A) := \sum_{\substack{f \in \mathcal{M}_n \\ f = A \mod Q}} \alpha_2(f). \tag{2.9}$$

The average of this sum $S_{\alpha_2;n;Q}(A)$ when we vary A over residue classes coprime to Q is

$$\langle S_{\alpha_2;n;Q} \rangle = \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f,Q)=1}} \alpha_2(f), \tag{2.10}$$

where $\Phi(Q)$ is the number of invertible residues modulo Q.

In Sect. 4 we will consider the variance of $S_{\alpha_2;n;Q}$ which is defined to be the average of the squared difference between $S_{\alpha_2;n;Q}$ and its mean value

$$\mathrm{Var}(S_{\alpha_2;n;Q}) = \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ (A,Q)=1}} |S_{\alpha_2;n;Q} - \langle S_{\alpha_2;n;Q} \rangle|^2. \tag{2.11}$$

proving the following theorem:

Theorem 2.1 *Let Q be a prime polynomial of degree bigger than 3, and set $N := \deg Q - 1$, then in the limit $q \to \infty$ the following holds:*

for $N \le n \le 2N+1$

$$\mathrm{Var}(S_{\alpha_2;n;Q}) \sim \frac{q^{\lfloor \frac{n}{2} \rfloor}}{\Phi(Q)},$$

for $2N+1 < n$ even

$$\mathrm{Var}(S_{\alpha_2;n;Q}) \sim \frac{q^n}{\Phi(Q)^2},$$

for $2N+1 < n$ odd

$$\mathrm{Var}(S_{\alpha_2;n;Q}) = O\left(\frac{q^{n-2}}{\Phi(Q)^2}\right).$$

Note that the restriction that Q is a prime is for simplicity only and we can also do the more general case of squarefree Q in the same way.

2.2 Short intervals

A "short interval" in $\mathbb{F}_q[x]$ is a set of the form

$$I(A;h) = \{f : ||f - A|| \le q^h\}, \tag{2.12}$$

where $A \in \mathcal{M}_n$ and $0 \le h \le n-2$. The norm is

$$||f|| := \#\mathbb{F}_q[t]/(f) = q^{\deg f}. \tag{2.13}$$

The cardinality of such a short interval is

$$\#I(A;h) = q^{h+1} =: H. \tag{2.14}$$

To facilitate comparison between statements for number field results and for function fields, we use a rough dictionary:

$$\begin{aligned} X &\leftrightarrow q^n \\ \log X &\leftrightarrow n \\ H &\leftrightarrow q^{h+1} \\ \log H &\leftrightarrow H+1 \end{aligned} \tag{2.15}$$

We define for $1 \le h < n$ and $A \in \mathcal{M}_n$

$$\mathcal{N}_{\alpha_2;h}(A) := \sum_{f \in I(A;h)} \alpha_2(f) \tag{2.16}$$

to be the number of square-full polynomials in the interval $I(A;h)$.

The mean value of $\mathcal{N}_{\alpha_2;h}$ when we average over $A \in \mathcal{M}_n$ is

$$\langle \mathcal{N}_{\alpha_2;h} \rangle := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \mathcal{N}_{\alpha_2;h}(A). \tag{2.17}$$

In Sect. 5 we will compute the variance of $\mathcal{N}_{\alpha_2;h}$

$$\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) := \frac{1}{q^n}\sum_{A\in\mathcal{M}_n} |\mathcal{N}_{\alpha_2;h}(A) - \langle \mathcal{N}_{\alpha_2;h}\rangle|^2 \tag{2.18}$$

proving the following theorem:

Theorem 2.2 *Set $N := n-h-2$, then in the limit $q\to\infty$ the following holds: for $0\le n\le 2N$*

$$\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) \sim \frac{H}{q^n}\cdot q^{\lfloor \frac{n}{2}\rfloor}, \tag{2.19}$$

for $2N < n \le 5N$

$$\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) \sim \frac{H}{q^n}\cdot q^{\left\lfloor \frac{n+N}{3}\right\rfloor}, \tag{2.20}$$

for $5N < n$

$$\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) \sim \frac{H}{q^n}\cdot q^{\frac{n+N}{6}}\cdot q^{\frac{-\lambda_n}{6}}, \tag{2.21}$$

where

$$\lambda_n = \begin{cases} 0 & n = 5N \mod 6,\\ 7 & n = 5N+1 \mod 6,\\ 6 & n = 5N+2 \mod 6,\\ 3 & n = 5N+3 \mod 6,\\ 4 & n = 5N+4 \mod 6,\\ 11 & n = 5N+5 \mod 6. \end{cases} \tag{2.22}$$

The conditions one needs to place on n in both Theorems 2.1 and 2.2 are not obvious to begin with. They will follow eventually because we express the variance in both cases in terms of zeros of L-functions, which are known to be polynomials in the function field settings.

3 Dirichlet characters and Katz's equidistribution results

3.1 Dirichlet characters

Let $Q(T)\in\mathbb{F}_q[T]$ be a polynomial of positive degree. A Dirichlet character modulo Q is a homomorphism

$$\chi : (\mathbb{F}_q[T]/(Q))^\times \to \mathbb{C}^\times. \tag{3.1}$$

One can extend χ to $\mathbb{F}_q[T]$ by defining it to vanish on polynomials which are not coprime to Q. We denote by $\Gamma(Q)$ the group of all Dirichlet characters modulo Q. Note that $|\Gamma(Q)|$ is the Euler totient function $\Phi(Q)$. A Dirichlet character needs then to satisfy the following: $\chi(fg)=\chi(f)\chi(g)$ for all $f,g\in\mathbb{F}_q[T]$, $\chi(1)=1$ and $\chi(f+hQ)=\chi(f)$ for all $f,h\in\mathbb{F}_q[T]$.

The orthogonality relations for Dirichlet characters are:

$$\frac{1}{\Phi(Q)}\sum_{\chi \bmod Q}\bar{\chi}(A)\chi(N) = \begin{cases} 1 & N = A \mod Q,\\ 0 & \text{otherwise.}\end{cases} \tag{3.2}$$

$$\frac{1}{\Phi(Q)}\sum_{A \bmod Q}\bar{\chi_1}(A)\chi_2(A) = \begin{cases} 1 & \chi_1=\chi_2,\\ 0 & \text{otherwise.}\end{cases} \tag{3.3}$$

A character χ is *primitive* if there is no proper divisor $Q'|Q$ such that $\chi(f) = 1$ whenever f is co-prime to Q and $f = 1 \mod Q'$. A character χ is called "even" if it acts trivially on the elements of $\mathbb{F}_q$, i.e. if $\chi(cf) = \chi(f)$ for all $0 \neq c \in \mathbb{F}_q$. Therefore, the number of even characters is given by $\Phi^{ev}(Q) = \frac{\Phi(Q)}{q-1}$. For example there are q^{m-1} even character mod T^m. Out of this there are $O(q^{m-2})$ nonprimitive even characters mod T^m (see subsection 3.3 in [13]) . A character is called "odd" if it is not even.

Define the following:

$\Gamma_{prim}(Q)$	the set of all primitive characters mod Q, $\Phi_{prim}(Q) := \|\Gamma_{prim}(Q)\|$.
$\Gamma^{ev}_{prim}(Q)$	the set of primitive even characters mod Q, $\Phi^{ev}_{prim}(Q) := \|\Gamma^{ev}_{prim}(Q)\|$.
$\Gamma^{odd}_{prim}(Q)$	the set of primitive odd characters mod Q, $\Phi^{odd}_{prim}(Q) := \|\Gamma^{odd}_{prim}(Q)\|$.
$\Gamma_{d\text{-}prim}(Q)$	the set of all characters χ mod Q such that χ^d (i.e. $\chi \times \cdots \times \chi$) is primitive for the fixed integer $d > 0$, $\Phi_{d\text{-}prim}(Q) := \|\Gamma_{d\text{-}prim}(Q)\|$. Note that this is a subset of $\Gamma_{prim}(Q)$.
$\Gamma^{d\text{-}odd}_{d\text{-}prim}(Q)$	the set of all characters χ mod Q such that χ^d is primitive and odd for the fixed integer $d > 0$, $\Phi^{d\text{-}odd}_{d\text{-}prim}(Q) := \|\Gamma^{d\text{-}odd}_{d\text{-}prim}(Q)\|$.

Next, we will check the proportion of the set $\Gamma_{d-prim}(Q)$ in the group of all characters mod Q ,$\Gamma(Q)$.

Lemma 3.1 *Let $Q \in \mathbb{F}_q[t]$ be a square-free polynomial, then in the limit of a large field size $q \to \infty$,*

$$\frac{\Phi_{d\text{-}prim}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right). \tag{3.4}$$

Proof By subsection (3.3) in [13] we have

$$\#(\Gamma(Q)/\Gamma_{prim}(Q)) \leq c \cdot q^{n-1} \tag{3.5}$$

for some constant c. Note that a character χ does not lie in $\Gamma_{d\text{-}prim}(Q)$ if χ^d does not lie in $\Gamma_{prim}(Q)$. In that case, χ^d lies in $\Gamma(Q)/\Gamma_{prim}(Q)$. Now consider the map $\chi \mapsto \chi^d$. Its kernel is of cardinality $\#\{\chi|\chi^d = 1\}$. Since every χ is a product of characters χ_j of $\mathbb{F}_q[T]/(f_j)$ when $Q = \prod_{j=1}^k f_j$, $\deg(f_j) = d_j$ and $\sum_{i=1}^k d_i = n$, the following bound holds:

$$\#\{\chi|\chi^d = 1\} \leq d^n. \tag{3.6}$$

Since every character χ such that χ^d is not primitive can be written as a product of a non primitive character and an element of the kernel, we get that $\#(\Gamma(Q)/\Gamma_{d\text{-}prim}(Q))$ can be at most $d^n \cdot c \cdot q^{n-1}$.

Now, if Q factors into k irreducible polynomials f_i of degree d_i, $\deg Q := n = \sum_{i=1}^k d_i$ then $\Phi(Q) = \prod_{i=1}^k (q^{d_i} - 1) \geq (q-1)^n$. It follows that $\Phi_{d-prim}(Q) \geq (q-1)^n - d^n \cdot c \cdot q^{n-1}$. Therefore, in the limit of $q \to \infty$ we get (3.4). □

Note that equation (3.25) in [13] asserts that as $q \to \infty$, almost all characters are **primitive** and **odd** in the sense that

$$\frac{\Phi^{odd}_{prim}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right). \tag{3.7}$$

Hence, exactly as before, we may also show that

Lemma 3.2 *Let $Q \in \mathbb{F}_q[t]$ be a square-free polynomial, then in the limit of a large field size $q \to \infty$,*

$$\frac{\Phi^{d\text{-}odd}_{d\text{-}prim}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right). \tag{3.8}$$

Next, we will prove a short lemma stating that under certain restrictions on the characteristic of the field, the primitivity of χ and χ^d is equivalent when χ is an even character mod T^m. This lemma will be useful later on in Sect. 5.

Lemma 3.3 *Let d be an integer co-prime to $\Phi(Q)$. Then the map $\chi \mapsto \chi^d$ is an automorphism of the group of characters mod Q, i.e. an automorphism of $\Gamma(Q)$.*

Proof The map is clearly an homomorphism since the group is abelian. Now, d is co-prime to the order of the group therefore there aren't any elements whose order dividing d and hence the kernel of the map is trivial. □

Lemma 3.4 *Let χ be an even Dirichlet character mod T^m, and let d be an integer s.t. $d < p$ when p is the characteristic of the field $\mathbb{F}_q$. Then χ is a primitive character if and only if χ^d is a primitive character.*

Proof The order of the subgroup of even characters mod T^m is $\Phi^{ev}(T^m) = q^{m-1}$. Taking $d < p$ when p is the characteristic of the field $\mathbb{F}_q$ gives d co-prime to $\Phi(T^m)$, in which case the above lemma applies. □

3.2 Dirichlet L-functions

Here we review some standard background concerning Dirichlet L-functions for the rational function field; see, for example [18], subsection 3.4 in [13], or section 6 in [14].

The L-function associated to a Dirichlet character $\chi \mod Q$ is defined as the following product over prime polynomials $P \in \mathbb{F}_q[T]$

$$L(u, \chi) = \prod_{P \nmid Q} (1 - \chi(P) u^{\deg P})^{-1}. \tag{3.9}$$

The product is absolutely convergent for $|u| < 1/q$. For $\chi = \chi_0$ the trivial character mod Q

$$L(u, \chi_0) = Z(u) \prod_{P \mid Q} (1 - u^{\deg P}). \tag{3.10}$$

If $Q \in \mathbb{F}_q[T]$ is a polynomial of degree $\deg Q \geq 2$ and χ is a nontrivial character mod Q, then the L-function associated to χ i.e. $L(u, \chi)$ is a polynomial in u of degree at most $\deg Q - 1$. If χ is even then $L(u, \chi)$ has a trivial zero at $u = 1$. Now, we may factor $L(u, \chi)$ in terms of the inverse roots

$$L(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j(\chi) u) \tag{3.11}$$

for which the Riemann hypothesis, proved by Weil, asserts that for each (nonzero) inverse root, either $|\alpha_j(\chi)| = 1$ or

$$|\alpha_j(\chi)| = q^{1/2}. \tag{3.12}$$

For a primitive odd character mod Q all the inverse roots have absolute value $q^{1/2}$. For a primitive even character mod Q all the inverse roots have absolute value $q^{1/2}$, except

for the trivial zero at 1. Thus, we may write $\alpha_j(\chi) = q^{1/2}\,\mathrm{e}^{i\Theta_j}$, and the L-function (for a primitive character χ) is

$$L(u,\chi) = (1-\lambda_\chi u)^{-1}\det(I - uq^{1/2}\Theta_\chi), \qquad \Theta_\chi = \mathrm{diag}(\mathrm{e}^{i\Theta_1},\ldots,\mathrm{e}^{i\Theta_N}). \tag{3.13}$$

where $N = \deg Q - 1$ and $\lambda_\chi = 0$ for odd character χ. For even χ we have $N = \deg Q - 2$ and $\lambda_\chi = 1$. The unitary matrix $\Theta_\chi \in U(N)$ determines a unique conjugacy class which is called the unitarized Frobenius matrix of χ.

3.3 Katz's equidistribution results

The main ingredients in our results on the variance are equidistribution and independence results for the Frobenii Θ_χ due to N. Katz.

Theorem 3.5 [9] *Fix $m \geq 4$. The unitarized Frobenii Θ_χ for the family of even primitive characters* mod T^{m+1} *become equidistributed in the projective unitary group $PU(m-1)$ of size $m-1$, as q goes to infinity.*

Theorem 3.6 [11] *If $m \geq 5$ and in addition the characteristics of the fields $\mathbb{F}_q$ are bigger than* 13*, then the set of conjugacy classes $(\Theta_{\chi^2}, \Theta_{\chi^3}, \Theta_{\chi^6})$, χ is even primitive character* mod T^{m+1}*, become equidistributed in the space of conjugacy classes of the product $PU(m-1)\times PU(m-1)\times PU(m-1)$ as q goes to infinity.*

For odd characters, the corresponding equidistribution and independence results are

Theorem 3.7 [10] *Fix $m \geq 2$. Suppose we are given a sequence of finite fields $\mathbb{F}_q$ and squarefree polynomials $Q(T) \in \mathbb{F}_q[T]$ of degree m. As $q \to \infty$, the conjugacy classes Θ_χ with χ running over all primitive odd characters modulo Q, are uniformly distributed in the unitary group $U(m-1)$.*

Theorem 3.8 [12] *If in addition we restrict the characteristics of the fields $\mathbb{F}_q$ is bigger than* 6*, then the set of conjugacy classes $(\Theta_{\chi^2}, \Theta_{\chi^3}, \Theta_{\chi^6})$ with χ running over all characters such that χ^2, χ^3, χ^6 are primitive odd characters modulo Q, become equidistributed in the space of conjugacy classes of the product $U(m-1)\times U(m-1)\times U(m-1)$ as q goes to infinity.*

4 The variance in arithmetic progressions

4.1 The mean value

Given a polynomial $Q \in \mathbb{F}_q[T]$ the average of $S_{\alpha_2;n;Q}(A)$ when we vary A over residue classes co-prime to Q (see (2.9)) equals to

$$\langle S_{\alpha_2;n;Q}\rangle = \frac{1}{\Phi(Q)}\sum_{\substack{f\in\mathcal{M}_n\\(f,Q)=1}}\alpha_2(f) = \frac{1}{\Phi(Q)}\sum_{f\in\mathcal{M}_n}\chi_0(f)\alpha_2(f) \tag{4.1}$$

To evaluate this consider the generating function

$$\frac{1}{\Phi(Q)}\sum_{\substack{f\in\mathcal{M}_n\\(f,Q)=1}}\alpha_2(f)u^n = \frac{1}{\Phi(Q)}\cdot\sum_{f\in\mathcal{M}_n}\chi_0(f)\alpha_2(f)u^n$$
$$= \frac{1}{\Phi(Q)}\cdot\frac{L(u^2,\chi_0)L(u^3,\chi_0)}{L(u^6,\chi_0)}$$

$$= \frac{1}{\Phi(Q)} \cdot \frac{Z(u^2)Z(u^3)}{Z(u^6)} \prod_{P|Q} \left(\frac{(1-u^{2\deg P})(1-u^{3\deg P})}{(1-u^{6\deg P})} \right)$$
$$= \frac{1}{\Phi(Q)} \cdot \frac{Z(u^2)Z(u^3)}{Z(u^6)} \prod_{P|Q} \left(\frac{(1-u^{2\deg P})}{(1+u^{3\deg P})} \right). \tag{4.2}$$

By expanding and comparing coefficients it is clear that the leading order coefficient in q (we are interested in $q \to \infty$) comes from $\frac{Z(u^2)Z(u^3)}{Z(u^6)}$. Therefore, by 2.8, we have

$$\langle S_{\alpha_2;n;Q} \rangle \sim \frac{q^{\lfloor n/2 \rfloor}}{\Phi(Q)}. \tag{4.3}$$

In the rest of this section we will evaluate the variance of $S_{\alpha_2;n;Q}$ i.e. the average of the squared difference between $S_{\alpha_2;n;Q}$ and its mean value.

4.2 The case of small n

See also subsection 4.2 in [14]. If $n < \deg Q$ then there is at most one polynomial $f \in \mathbb{F}_q[T]$ of degree n such that $f = A \mod Q$. In this case, when $q \to \infty$

$$Var(S_{\alpha_2;n;Q}) \sim \frac{q^n}{\Phi(Q)} \langle \alpha_2 \rangle_n. \tag{4.4}$$

Indeed, if $n < \deg Q$ we can use (4.3) to see that

$$|\langle S_{\alpha_2;n;Q} \rangle| \ll_n \frac{1}{q^{n/2}}. \tag{4.5}$$

Hence

$$\begin{aligned} Var(S_{\alpha_2;n;Q}) &= \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ (A,Q)=1}} |S_{\alpha_2;n;Q}(A)|^2 \left(1 + O\left(\frac{1}{q^{n/2}}\right)\right) \\ &= \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f,Q)=1}} |\alpha_2(f)|^2 \left(1 + O\left(\frac{1}{q^{n/2}}\right)\right) \\ &\sim \frac{q^n}{\Phi(Q)} \langle \alpha_2 \rangle_n \\ &\sim \frac{q^{\lfloor n/2 \rfloor}}{\Phi(Q)}. \end{aligned} \tag{4.6}$$

4.3 A formula for the variance

We present a formula for the variance of $S_{\alpha_2;n;Q}$ using Dirichlet characters [14, §4.1]. We start with the following expansion, using the first orthogonality relation for Dirichlet characters (see (3.2)) to pick out an arithmetic progression:

$$S_{\alpha_2,n,Q}(A) = \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f,Q)=1}} \alpha_2(f) + \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0} \overline{\chi(A)} \mathcal{M}(n; \alpha_2 \chi), \tag{4.7}$$

where

$$\mathcal{M}(n; \alpha_2 \chi) := \sum_{f \in M_n} \alpha_2(f) \chi(f). \tag{4.8}$$

Note that the contribution of the trivial character is equal to the average of $S_{\alpha_2;n;Q}(A)$. Therefore

$$S_{\alpha_2;n;Q} - \langle S_{\alpha_2;n;Q} \rangle = \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0 \bmod Q} \overline{\chi}(A) \mathcal{M}(n; \alpha_2 \chi). \tag{4.9}$$

Using the above and the second orthogonality relation for Dirichlet characters (see (3.3)), we have the following expression for the variance:

$$Var(S_{\alpha_2;n;Q}) = \langle |S_{\alpha_2;n;Q} - \langle S_{\alpha_2;n;Q}\rangle|^2\rangle = \frac{1}{\Phi(Q)^2}\sum_{\chi\neq\chi_0}|\mathcal{M}(n;\alpha_2\chi)|^2. \tag{4.10}$$

4.4 The quadratic character and the cubic character

Next, we evaluate $\mathcal{M}(n;\alpha_2\chi)$ for $\chi = \chi_2$ a quadratic character and for $\chi = \chi_3$ a cubic character. We assume here for simplicity that Q is prime polynomial. The sum $\mathcal{M}(n;\alpha_2\chi)$ given by (4.8), is the coefficient of u^n in the expansion of $\frac{L(u^2,\chi^2)L(u^3,\chi^3)}{L(u^6,\chi^6)}$. Thus for $\chi = \chi_2$, the generating function of $\mathcal{M}(n;\alpha_2\chi_2)$ has the following form:

$$L(u^3,\chi_2)\cdot\frac{Z(u^2)(1-u^{2\deg Q})}{Z(u^6)(1-u^{6\deg Q})} \tag{4.11}$$

recall that

$$Z(u) = \frac{1}{1-qu} \tag{4.12}$$

and that

$$L(u,\chi) = \prod_{j=1}^{\deg Q-1}(1-\alpha_j(\chi)u), \tag{4.13}$$

therefore by expanding and comparing coefficients while bearing in mind the Riemann hypothesis (3.12), we can see that for an even n the leading order coefficient in q come from $Z(u^2)$ and for odd n it comes from $Z(u^2)$ and $L(u^3,\chi_2)$. Thus we get

$$\mathcal{M}(n;\alpha_2\chi_2)\sim\begin{cases} q^{\frac{n}{2}} & n \text{ even},\\ -q^{\frac{n-3}{2}}\cdot\sum_{j=1}^{\deg Q-1}\alpha_j(\chi_2) & n \text{ odd},\end{cases} \tag{4.14}$$

where $\alpha_j(\chi_2)$ are the inverse roots of $L(u,\chi_2)$.

For $\chi = \chi_3$, the generating function of $\mathcal{M}(n;\alpha_2\chi_3)$ has the following form:

$$L(u^2,\chi_3^2)\cdot\frac{Z(u^3)(1-u^{3\deg Q})}{Z(u^6)(1-u^{6\deg Q})} \tag{4.15}$$

as before we get

$$\mathcal{M}(n;\alpha_2\chi_3)\sim\begin{cases} q^{\frac{n}{3}} & n=0 \mod 3,\\ q^{\frac{n-4}{3}}\cdot\sum_{j,l=1}^{\deg Q-1}\alpha_j(\chi_3)\alpha_l(\chi_3) & n=1 \mod 3,\\ -q^{\frac{n-2}{3}}\cdot\sum_{j=1}^{\deg Q-1}\alpha_j(\chi_3) & n=2 \mod 3,\end{cases} \tag{4.16}$$

where $\alpha_j(\chi_3)$ are the inverse roots of $L(u,\chi_3)$.

4.5 Average of the sum $\mathcal{M}(n;\alpha_2\chi)$

Lemma 4.1 *For a Dirichlet character χ mod Q, such that χ^2, χ^3, χ^6 are odd and primitive*

$$\mathcal{M}(n;\alpha_2\chi) = \sum_{\substack{2j+3l+6k=n\\ 0\le j\le N\\ 0\le l\le N\\ 0\le k}} q^{\frac{j+k+l}{2}}\operatorname{tr}\Lambda_j(\Theta_{\chi^2})\operatorname{tr}\Lambda_l(\Theta_{\chi^3})\operatorname{tr}\operatorname{Sym}^k(\Theta_{\chi^6}), \tag{4.17}$$

where $N := \deg Q-1$, $\Theta_\chi \in U(N)$ is the unitarized Frobenius matrix, Sym^n *is the symmetric $n-$th power representation, and Λ_n is the exterior $n-$th power representation.*

For $\chi \neq \chi_0, \chi_2, \chi_3$ mod Q, the following bound holds:

$$|\mathcal{M}(n;\alpha_2\chi)| \ll_{\deg Q} \sum_{\substack{2j+3l+6k=n \\ 0\le j\le N \\ 0\le l\le N \\ 0\le k}} q^{\frac{j+k+l}{2}}. \tag{4.18}$$

Proof The sum $\mathcal{M}(n;\alpha_2\chi)$ given by (4.8), is the coefficient of u^n in the expansion of $\frac{L(u^2,\chi^2)L(u^3,\chi^3)}{L(u^6,\chi^6)}$. For an odd primitive characters χ mod Q, we use the Riemann Hypothesis (3.12) (Weil's theorem) to write

$$L(u,\chi) = \det(I - uq^{\frac{1}{2}}\Theta_\chi). \tag{4.19}$$

Since the coefficients of the characteristic polynomial of an $N\times N$ matrix with eigenvalues $\lambda_1,\ldots,\lambda_n$ are the elementary symmetric functions $\sum_{1\le i_1<\ldots<i_r}\lambda_{i_1}\cdots\lambda_{i_r}$ which give the character of the exterior power representation, we may write

$$L(u,\chi) = \sum_{i=0}^{\deg Q-1} u^i q^{i/2}\,\mathrm{tr}\,\Lambda_i(\Theta_\chi) \tag{4.20}$$

and in the same way

$$\frac{1}{L(u,\chi)} = \frac{1}{\det(I-uq^{\frac{1}{2}}\Theta_\chi)} = \sum_{i=0}^{\infty} u^i q^{i/2}\,\mathrm{tr}\,\mathrm{Sym}^i(\Theta_\chi). \tag{4.21}$$

Abbreviate as follows:

$$\Lambda_i(\chi) := \mathrm{tr}\,\Lambda_i(\Theta_\chi), \qquad \mathrm{Sym}^i(\chi) = \mathrm{tr}\,\mathrm{Sym}^i(\Theta_\chi)$$

to have

$$\frac{L(u^2,\chi^2)L(u^3,\chi^3)}{L(u^6,\chi^6)} = \sum_{j=0}^{\deg Q-1}\sum_{l=0}^{\deg Q-1}\sum_{k=0}^{\infty} u^{2j+3l+6k} q^{\frac{j+k+l}{2}} \Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6). \tag{4.22}$$

Hence the coefficient of u^n is indeed given by (4.17).

For $\chi \neq \chi_0, \chi_2, \chi_3$ mod Q for which at least one of χ^2, χ^3, χ^6 is not primitive or not odd, we still have $L(u,\chi) = \prod_{j=1}^{\deg Q-1}(1-\alpha_j(\chi)u)$ with all the inverse roots $|\alpha_j(\chi)| = q^{\frac{1}{2}}$ or $|\alpha_j(\chi)| = 1$, and hence we obtain (4.18). □

Next, we want to evaluate $\sum_{\substack{2j+3l+6k=n \\ 0\le j\le N \\ 0\le l\le N \\ 0\le k}} q^{j+k+l}$. Denote

$$S(n) := \sum_{\substack{2j+3l+6k=n \\ 0\le j\le N \\ 0\le l\le N \\ 0\le k}} q^{j+k+l}. \tag{4.23}$$

Lemma 4.2 *Let $N := \deg Q - 1$ then in the limit $q\to\infty$,*
for $0 \le n \le 2N$

$$S(n) \sim q^{\lfloor \frac{n}{2} \rfloor}, \tag{4.24}$$

for $2N < n \le 5N$

$$S(n) \sim q^{\left\lfloor \frac{n+N}{3} \right\rfloor}, \tag{4.25}$$

for $5N < n$

$$S(n) \sim q^{\frac{n+N}{6}} \cdot q^{\frac{-\lambda_n}{6}}, \tag{4.26}$$

where

$$\lambda_n = \begin{cases} 0 & n = 5N \mod 6, \\ 7 & n = 5N+1 \mod 6, \\ 6 & n = 5N+2 \mod 6, \\ 3 & n = 5N+3 \mod 6, \\ 4 & n = 5N+4 \mod 6, \\ 11 & n = 5N+5 \mod 6. \end{cases} \tag{4.27}$$

Proof In order to find the leading order term of $S(n)$ we need first to take the maximal possible j and then the maximal possible l which satisfy $2j+3l+6k = n, 0 \le j \le N, 0 \le l \le N$ (note that k will then be determined).

In the first case $0 \le n \le 2N$ if 2 divides n then $j = n/2, l = 0, k = 0$ will clearly give the leading order term. If 2 does not divide n then $j = (n-3)/2, l = 1, k = 0$ will give the leading order term.

In the second case $2N < n \le 5N$, we write $j = N - i_j$ and then we have $n - 2N = 6k + 3l - 2i_j$ and so clearly the values for k, l, i_j that will give the leading order term, depend on the value of $n - 2N \mod 3$ (or equivalently $n + N \mod 3$). Here our first priority is to minimize i_j and then to maximize l. The leading order term will be given by $q^{\frac{n+N-i_j}{3} - \frac{k}{2}}$ which gives $q^{\left\lfloor \frac{n+N}{3} \right\rfloor}$.

In the last case $5N < n$, we write $j = N - i_j$ and $l = N - i_l$, then we have $n - 5N = 6k - 3i_l - 2i_j$ and so clearly the values for k, i_l, i_j that will give the leading order term, depend on the value of $n - 5N \mod 6$. Here our first priority is to minimize i_j and then to minimize i_l. The leading order term will be given by $q^{\frac{n+7N-3i_l-4i_j}{6}}$. Note that in the notations of Eqs. (4.26) and (4.27) we have $4i_j + 3i_l = \lambda_n$ □

4.6 Proof of Theorem 2.1

Recall that by Lemma 3.2, we have that the number of characters which are not in $\Gamma_{d-prim}^{d-odd}(Q)$ is $O(\frac{\Phi(Q)}{q})$ when $q \to \infty$. Therefore, by using the formula for the variance that was given in (4.10) we may write

$$Var(S_{\alpha_2;n;Q}) = \frac{1}{\Phi(Q)^2} \sum_{\substack{\chi \neq \chi_0 \\ \chi \in \Gamma_{6-prim}^{6-odd}(Q)}} |\mathcal{M}(n;\alpha_2\chi)|^2 + \frac{1}{\Phi(Q)^2}|\mathcal{M}(n;\alpha_2\chi_2)|^2 + \lambda_3 \frac{1}{\Phi(Q)^2}|\mathcal{M}(n;\alpha_2\chi_3)|^2 + O\left(\frac{S(n)}{\Phi(Q)q}\right), \tag{4.28}$$

where $\lambda_3 = 2$ if $|Q| = 1 \mod 3$, and zero otherwise. Note that we assume Q is prime and that the characteristic of the field $\mathbb{F}_q$ is odd therefore there is one quadratic character mod Q and either two or zero cubic characters, depending on whether $|Q| = 1 \mod 3$ or not.

For the first sum in (4.28), use (4.17) to have

$$\frac{1}{\Phi(Q)^2}\sum_{\substack{\chi\neq\chi_0\\ \chi\in\Gamma_{6-prim}^{6-odd}(Q)}}|\mathcal{M}(n;\alpha_2\chi)|^2$$

$$=\frac{1}{\Phi(Q)^2}\sum_{\substack{\chi\neq\chi_0\\ \chi\in\Gamma_{6-prim}^{6-odd}(Q)}}\left|\sum_{\substack{2j+3l+6k=n\\ 0\le j\le N\\ 0\le l\le N\\ 0\le k}} q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6)\right|^2. \tag{4.29}$$

We can use now the equidistribution result given in Theorem 3.8, to have

$$\frac{1}{\Phi(Q)^2}\sum_{\substack{\chi\neq\chi_0\\ \chi\in\Gamma_{6-prim}^{6-odd}(Q)}}\left|\sum_{\substack{2j+3l+6k=n\\ 0\le j\le N\\ 0\le l\le N\\ 0\le k}} q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6)\right|^2$$

$$\sim\frac{1}{\Phi(Q)}\iiint_{U(N)}\left|\sum_{\substack{2j+3l+6k=n\\ 0\le j\le N\\ 0\le l\le N\\ 0\le k}} q^{\frac{j+k+l}{2}}\operatorname{tr}\Lambda_j(U_1)\operatorname{tr}\Lambda_l(U_2)\operatorname{tr}\mathrm{Sym}^k(U_3)\right|^2 dU_1\,dU_2\,dU_3$$

$$=\frac{1}{\Phi(Q)}\sum_{\substack{2j_1+3l_1+6k_1=n\\ 2j_1+3l_1+6k_1=n\\ 0\le j_1,j_2\le N\\ 0\le l_1,l_2\le N\\ 0\le k_1,k_2}} q^{\frac{j_1+k_1+l_1+j_2+k_2+l_2}{2}}\times\int_{U(N)}\operatorname{tr}\Lambda_{j_1}(U_1)\overline{\operatorname{tr}\Lambda_{j_2}(U_1)}\,dU_1$$

$$\times\int_{U(N)}\operatorname{tr}\Lambda_{l_1}(U_2)\overline{\operatorname{tr}\Lambda_{l_2}(U_2)}\,dU_2\times\int_{U(N)}\operatorname{tr}\mathrm{Sym}^{k_1}(U_3)\overline{\operatorname{tr}\mathrm{Sym}^{k_2}(U_3)}\,dU_3 \tag{4.30}$$

It is well known that Λ_j are distinct irreducible representations of the unitary group $U(N)$, and hence one gets

$$\int_{U(N)}\operatorname{tr}\Lambda_j(U)\overline{\operatorname{tr}\Lambda_i(U)}dU=\delta_{j,i}. \tag{4.31}$$

It is also well known that Sym^j are distinct irreducible representations of the unitary group $U(N)$, hence

$$\int_{U(N)}\operatorname{tr}\mathrm{Sym}^j(U)\overline{\operatorname{tr}\mathrm{Sym}^i(U)}dU=\delta_{j,i}. \tag{4.32}$$

Therefore

$$\frac{1}{\Phi(Q)^2}\sum_{\substack{\chi\neq\chi_0\\ \chi\in\Gamma_{6-prim}^{6-odd}(Q)}}|\mathcal{M}(n;\alpha_2\chi)|^2\sim\frac{1}{\Phi(Q)}\sum_{\substack{2j+3l+6k=n\\ 0\le j\le N\\ 0\le l\le N\\ 0\le k}} q^{j+k+l}. \tag{4.33}$$

The contribution from the second and third summands was evaluated in Subsect. 4.4. Adding up everything and checking for the leading order terms by using Lemma 4.2 finishes the proof.

5 The variance over short intervals

5.1 The mean value

The mean value of $\mathcal{N}_{\alpha_2;h}$ when we average over $A \in \mathcal{M}_n$ is

$$\begin{aligned}\langle \mathcal{N}_{\alpha_2;h} \rangle &:= \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \mathcal{N}_{\alpha_2;h}(A) \\ &= \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \sum_{f \in I(A;h)} \alpha_2(f) \\ &= q^{h+1} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha_2(f) \\ &= q^{h+1} \langle \alpha_2 \rangle_n. \end{aligned} \tag{5.1}$$

By (2.8) we have in the limit $q \to \infty$

$$\langle \mathcal{N}_{\alpha_2;h} \rangle \sim H \cdot q^{\lfloor n/2 \rfloor - n}, \tag{5.2}$$

where $H = \#I(A;h) = q^{h+1}$. In the rest of this section we will evaluate the variance of $\mathcal{N}_{\alpha_2;h}$ i.e. the average of the squared difference between $\mathcal{N}_{\alpha_2;h}$ and its mean value.

5.2 An expression for the variance

To begin the proof of Theorem 2.2, we express the variance of the short interval sums $\mathcal{N}_{\alpha_2;h}$ in terms of sums of the function α_2, twisted by primitive even Dirichlet characters, similarly to what was done in the previous section.

Lemma 5.1 *As $q \to \infty$*

$$\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) = \frac{H}{q^n} \frac{1}{\Phi^{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi \neq \chi_0 \text{ even}}} \sum_{\substack{m_1,m_2=0 \\ m_1,m_2 \neq n-1}}^{n} \mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}, \tag{5.3}$$

where the definition of $\mathcal{M}(n;\alpha_2\chi)$ was first given in (4.8)

$$\mathcal{M}(n;\alpha_2\chi) := \sum_{f \in M_n} \alpha_2(f)\chi(f)\,. \tag{5.4}$$

Proof To compute the variance, we use [14, Lemma 5.4] which gives an expression for the variance of sums over short intervals of certain arithmetic functions α which are "even" ($\alpha(cf) = \alpha(f)$ for $c \in \mathbb{F}_q^\times$), multiplicative, and symmetric under the map $f^*(t) := t^{\deg f} f(\frac{1}{t})$, in the sense that

$$\alpha(f^*) = \alpha(f), \quad \text{if } f(0) \neq 0\,. \tag{5.5}$$

Since the indicator function for square full polynomials α_2 clearly satisfies all of these conditions, we may use [14, Lemma 5.4] to obtain

$$\begin{aligned}\mathrm{Var}(\mathcal{N}_{\alpha_2;h}) = \frac{H}{q^n} &\sum_{m_1,m_2=0}^{n} \alpha_2(T^{n-m_1})\overline{\alpha_2(T^{n-m_2})} \\ &\times \frac{1}{\Phi^{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi \neq \chi_0 \text{ even}}} \mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}. \end{aligned} \tag{5.6}$$

By the definition of α_2 we have $\alpha_2(T^{n-m}) = 1$ when $m \neq n-1$ and $\alpha_2(T^{n-m}) = 0$ when $m = n-1$, hence (5.3) follows. □

To compute the variance, we need to obtain an expression for $\mathcal{M}(n;\alpha_2\chi)$. Consider the generating function

$$\sum_{n=0}^{\infty}\mathcal{M}(n;\alpha_2\chi)u^n=\frac{L(u^2,\chi^2)L(u^3,\chi^3)}{L(u^6,\chi^6)}. \tag{5.7}$$

For an even primitive characters $\chi \bmod T^{n-h}$, $L(u,\chi)$ has a trivial zero at $u=1$, hence we may write

$$L(u,\chi)=(1-u)\det(I-uq^{\frac{1}{2}}\Theta_\chi)=(1-u)\sum_{i=0}^{n-h-2}u^iq^{i/2}\operatorname{tr}\Lambda_i(\Theta_\chi) \tag{5.8}$$

and

$$\frac{1}{L(u,\chi)}=\frac{1}{(1-u)\det(I-uq^{\frac{1}{2}}\Theta_\chi)}=\frac{1}{(1-u)}\sum_{i=0}^{\infty}u^iq^{i/2}\operatorname{tr}Sym^i(\Theta_\chi). \tag{5.9}$$

Therefore, the generating function of $\mathcal{M}(n;\alpha_2\chi)$(i.e. $\frac{L(u^2,\chi^2)L(u^3,\chi^3)}{L(u^6,\chi^6)}$) for $\chi \bmod T^{n-h}$ such that χ^2,χ^3,χ^6 are primitive and even can be written as follows:

$$\begin{aligned}&\frac{(1-u^2)(1-u^3)\det(I-u^2q^{\frac{1}{2}}\Theta_{\chi^2})\det(I-u^3q^{\frac{1}{2}}\Theta_{\chi^3})}{(1-u^6)\det(I-u^6q^{\frac{1}{2}}\Theta_{\chi^6})}\\&=\frac{(1-u^2)}{(1+u^3)}\sum_{j=0}^{n-h-2}\sum_{l=0}^{n-h-2}\sum_{k=0}^{\infty}u^{2j+3l+6k}q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6).\end{aligned} \tag{5.10}$$

By expanding and comparing coefficients we have

$$\mathcal{M}(m;\alpha_2\chi)=\mathcal{S}'_\chi(m)-\mathcal{S}'_\chi(m-2), \tag{5.11}$$

where for $1\neq m\geq 0$

$$\mathcal{S}'_\chi(m):=\sum_{\substack{2j+3l+6k+3i=m\\0\leq j,l\leq n-h-2\\0\leq k,i}}(-1)^iq^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6) \tag{5.12}$$

and

$$\mathcal{S}'_\chi(1),\mathcal{S}'_\chi(-1),\mathcal{S}'_\chi(-2):=0. \tag{5.13}$$

Now back to the variance formula (see (5.3)), we can split the sum into two parts: the sum over $\chi\neq\chi_0 \bmod T^{n-h}$, $\chi\in\Gamma^{ev}_{prim}(T^{n-h})$ and the sum over even non-primitive characters mod T^{n-h}. We start by considering the first sum which will give the main term since most of the even characters are also primitive. With the second sum which will give an error term we deal later. Note: by Lemma 3.4 it is enough to split to these sums, and we can still use (5.9) and (5.8) for χ^2,χ^3,χ^6.

For χ even and primitive, consider the inner sum in the variance formula:

$$\begin{aligned}&\sum_{\substack{m_1,m_2=0\\m_1,m_2\neq n-1}}^{n}\mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}\\&=\sum_{m_1,m_2=0}^{n-2}\mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}+|\mathcal{M}(n;\alpha_2\chi)|^2\\&\quad+\overline{\mathcal{M}(n;\alpha_2\chi)}\sum_{m=0}^{n-2}\mathcal{M}(m;\alpha_2\chi)+\mathcal{M}(n;\alpha_2\chi)\sum_{m=0}^{n-2}\overline{\mathcal{M}(m;\alpha_2\chi)}.\end{aligned} \tag{5.14}$$

The sum over $\mathcal{M}(m;\alpha_2\chi)$ equals

$$\sum_{m=0}^{n-2}\mathcal{M}(m;\alpha_2\chi)=\sum_{m=0}^{n-2}(\mathcal{S}'_{\chi}(m)-\mathcal{S}'_{\chi}(m-2))$$
$$=(\mathcal{S}'_{\chi}(n-2)+\mathcal{S}'_{\chi}(n-3)). \tag{5.15}$$

Hence we get

$$\sum_{\substack{m_1,m_2=0\\ m_1,m_2\neq n-1}}^{n}\mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}=|\mathcal{S}'_{\chi}(n)|^2+|\mathcal{S}'_{\chi}(n-3)|^2+\mathcal{S}'_{\chi}(n-3)\overline{\mathcal{S}'_{\chi}(n)}$$
$$+\overline{\mathcal{S}'_{\chi}(n-3)}\mathcal{S}'_{\chi}(n). \tag{5.16}$$

By the definition of $\mathcal{S}'_{\chi}(n)$ (see (5.12)) we may rewrite it for $n\geq 3$ in the following way

$$\mathcal{S}'_{\chi}(n)=\sum_{\substack{2j+3l+6k+3i=n-3\\ 0\leq j,l\leq n-h-2\\ 0\leq k\\ -1\leq i}}(-1)^{i+1}q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6). \tag{5.17}$$

Now split the above into two sums, the sum over $i\geq 0$ and the sum over $i=-1$

$$\sum_{\substack{2j+3l+6k=n\\ 0\leq j,l\leq n-h-2\\ 0\leq k}}q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6)$$
$$-\sum_{\substack{2j+3l+6k+3i=n-3\\ 0\leq j,l\leq n-h-2\\ 0\leq k,i}}(-1)^i q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6). \tag{5.18}$$

Denote the first sum by $H_{\chi}(n)$

$$H_{\chi}(n):=\sum_{\substack{2j+3l+6k=n\\ 0\leq j,l\leq n-h-2\\ 0\leq k}}q^{\frac{j+k+l}{2}}\Lambda_j(\chi^2)\Lambda_l(\chi^3)Sym^k(\chi^6) \tag{5.19}$$

to have

$$\mathcal{S}'_{\chi}(n)=H_{\chi}(n)-\mathcal{S}'_{\chi}(n-3). \tag{5.20}$$

By plugging this into (5.16) we can see that most of the terms cancel and we are left only with

$$\sum_{\substack{m_1,m_2=0\\ m_1,m_2\neq n-1}}^{n}\mathcal{M}(m_1;\alpha_2\chi)\overline{\mathcal{M}(m_2;\alpha_2\chi)}=|H_{\chi}(n)|^2. \tag{5.21}$$

Hence the contribution from even primitive characters to the variance formula (see (5.3)) is

$$\frac{H}{q^n}\frac{1}{\Phi^{ev}(T^{n-h})}\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}|H_{\chi}(n)|^2. \tag{5.22}$$

Note that there is a unique solution to $2j+3l+6k=n$, $0\le j,l\le n-h-2$, $0\le k$ that maximizes the quantity $j+l+k$ (Lemma 4.2). Denote this solution by j',l',k', to have

$$\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}|H_\chi(n)|^2=\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}q^{j'+l'+k'}|\Lambda_{j'}(\chi^2)\Lambda_{l'}(\chi^3)Sym^{k'}(\chi^6)|^2+\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}g(\chi,j',l',k'),\tag{5.23}$$

where $g(\chi,j',l',k')$ is defined to be the sum over all the other terms. Clearly $g(\chi,j',l',k')$ is of lower order of q by the choice of j',l',k' therefore its contribution is negligible. The first term here will give the main term in the variance expression. By using the equidistribution result (Theorem 3.6) we get

$$\begin{aligned}&\frac{1}{\Phi^{ev}(T^{n-h})}\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}|\Lambda_{j'}(\chi^2)\Lambda_{l'}(\chi^3)Sym^{k'}(\chi^6)|^2\\ &\sim\iiint_{PU(n-h-2)}|\operatorname{tr}\Lambda_{j'}(U_1)\operatorname{tr}\Lambda_{l'}(U_2)\operatorname{tr}\mathrm{Sym}^{k'}(U_3)|^2\,dU_1\,dU_2\,dU_3.\end{aligned}\tag{5.24}$$

We may pass from the projective unitary group $PU(n-h-2)$ to the unitary group because the function $|\operatorname{tr}\Lambda_{j'}(U_1)\operatorname{tr}\Lambda_{l'}(U_2)\operatorname{tr}\mathrm{Sym}^{k'}(U_3)|^2$ being averaged is invariant under scalar multiplication. Then, by (4.31) and (4.32), we conclude that the contribution of the first term to the variance is

$$\frac{H}{q^n}\frac{1}{\Phi^{ev}(T^{n-h})}\sum_{\substack{\chi \bmod T^{n-h}\\ \chi\neq\chi_0\in\Gamma^{ev}_{prim}}}q^{j'+l'+k'}|\Lambda_{j'}(\chi^2)\Lambda_{l'}(\chi^3)Sym^{k'}(\chi^6)|^2\sim\frac{H}{q^n}q^{j'+l'+k'}\tag{5.25}$$

this combined with Lemma 4.2 (with $N=n-h-2$) gives the main term.

Now, in order to complete the proof, it remains to bound the contribution of the even characters which are non-primitive to the variance. Note that we do not have quadratic or cubic characters here since $\Phi^{ev}(T^m)=q^{m-1}$ and we are considering the case of characteristic bigger than 13 (see Theorem 3.6), therefore there cannot be any even characters mod T^m of order 2 or 3. For even characters which are non-primitive we still have the bound (4.18) with $N=n-h-2$, and since their proportion is $O(1/q)$ in the set of even characters, then we can bound their contribution as in the previous section, therefore we skip the verification.

Acknowledgements

The author gratefully acknowledges support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms. The author would like to thank Zeev Rudnick for suggesting this problem and to both Jon Keating and Zeev Rudnick for helpful discussions and remarks. The author would also like to thank Ofir Gorodetsky for an important observation, and to the referees for their comments.

Competing interests

The author declares that she has no competing interests.

Received: 12 May 2016 Accepted: 23 November 2016
Published online: 17 January 2017

References

1. Bateman, P.T., Grosswald, E.: On a theorem of Erds and Szekeres. Ill. J. Math. **2**(1), 88–98 (1958)
2. Cai, Y.: On the distribution of square-full integers. Acta Math. Sinica (N.S.) **13**, 269-280 (1997). **(A Chinese summary appears in Acta Math. Sinica 40 (1997), 480)**

3. Cao, X.-D.: The distribution of square-full integers. Period. Math. Hung. **28**, 43–54 (1994)
4. Cao, X.: On the distribution of square-full integers. Period. Math. Hung. **34**, 169–175 (1997)
5. Erdös, P., Szekeres, G.: *Ü*ber die Anzahl der Abelschen Gruppen gegebener Ordnung und *ü*ber ein verwandtes zahlentheoretisches problem. Acta. Sci. Math. **7**, 95–102 (1935)
6. Filaseta, M., Trifonov, O.: The distribution of fractional parts with applications to gap results in number theory. Proc. Lond. Math. Soc. **73**(2), 241–278 (1996)
7. Heath-Brown, D.R.: Square-full numbers in short intervals. In: Math. Proc. Cambridge Philos. Soc, vol. 110, no. 1, pp. 1–3. Cambridge University Press, Cambridge (1991)
8. Huxley, M.N., Trifonov, O.: The square-full numbers in an interval. In: Mathematical Proceedings of the Cambridge Philosophical Society, vol. 119, pp. 201–208. Cambridge Philosophical Society, Cambridge (1996)
9. Katz, N.M.: Witt vectors and a question of Keating and Rudnick. Int. Math. Res. Not. IMRN **2013**(16), 3613–3638 (2013)
10. Katz, N.: On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor. Int. Math. Res. Not. IMRN **2013**(14), 3221–3249 (2013)
11. Katz, N.: Witt vectors and a question of Entin, Keating, and Rudnick. Int. Math. Res. Not. IMRN **2015**(14), 5959–5975 (2015). doi:10.1093/imrn/rnu120
12. Katz, N.: On two questions of Entin, Keating, and Rudnick on primitive Dirichlet characters. Int. Math. Res. Not. IMRN **2015**(15), 6044–6069 (2015). doi:10.1093/imrn/rnu121
13. Keating, J.P., Rudnick, Z.: The variance of the number of prime polynomials in short intervals and in residue classes. Int. Math. Res. Not **2012**, 259–288 (2012). doi:10.1093/imrn/rns220
14. Keating, J., Rudnick, Z.: Squarefree polynomials and Möbius values in short intervals and arithmetic progressions. Algebra Number Theory **10**, 375–420 (2016)
15. Liu, H.-Q.: The distribution of square-full integers. Ark. Mat. **32**, 449–454 (1994)
16. Liu, H.-Q.: The number of squarefull numbers in an interval. Acta Arith. **64**(2), 129–149 (1993)
17. Munsch, M.: Character sums over squarefree and squarefull numbers. Arch. Math. **102**(6), 555–563 (2014)
18. Rosen, M.: Number theory in function fields. Graduate texts in mathematics 210. Springer, New York (2002)
19. Suryanarayana, D., Sitamachandra, R.: The distribution of square-full integers. Ark. Mat. **11**, 195–201 (1973)
20. Wu, J.: On the distribution of square-full integers. Arch. Math. **77**, 233–240 (2001)
21. Wu, J.: On the distribution of square-full and cube-full integers. Monatsh. Math. **126**, 353–367 (1998)
22. Zhu, W., Yu, K.: The distribution of square-full integers. Pure Appl. Math. **12**, 113–122 (1996)